(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 198 11 720 A 1**

(51) Int. Cl.[6]: H 04 L 9/32

(21) Aktenzeichen: 198 11 720.5
(22) Anmeldetag: 18. 3. 98
(43) Offenlegungstag: 30. 9. 99

DE 198 11 720 A 1

(71) Anmelder:
Kobil Computer GmbH, 67547 Worms, DE

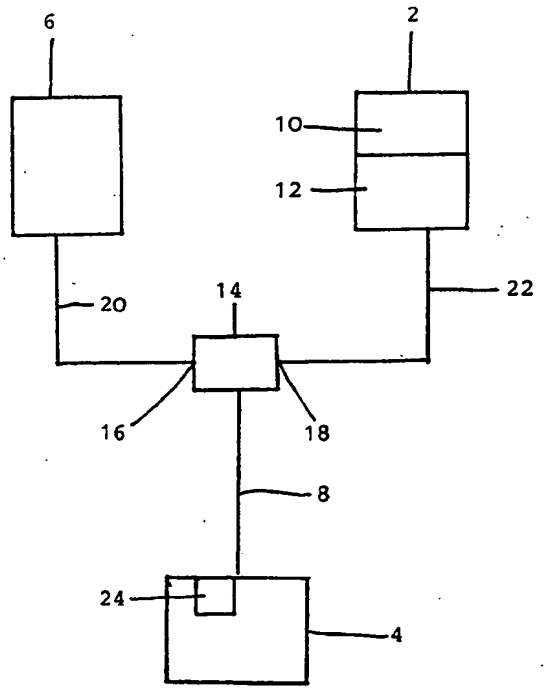
(72) Erfinder:
Koyun, Ismet, 67547 Worms, DE

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Vorrichtung zum Erstellen einer digitalen Signatur

(57) Eine Vorrichtung zum Erstellen einer digitalen Signatur enthält einen Computer (4) und ein externes Ausgabegerät (6). Die Vorrichtung soll dahingehend weitergebildet werden, daß ein Benutzer sicher sein kann, nur das von ihm gewünschte Dokument zu signieren und nichts anderes. Es wird vorgeschlagen, zwischen dem Computer (4), insbesondere dessen Zentraleinheit, und dem externen Ausgabegerät (6) ein sicheres Modul (2) zur Berechnung der digitalen Signatur mit Hilfe eines Secret Key anzuordnen.



DE 198 11 720 A 1

Beschreibung

Die Erfindung bezieht sich auf eine Vorrichtung zum Erstellen einer digitalen Signatur gemäß den im Oberbegriff des Patentanspruchs 1 angegebenen Merkmalen.

In zunehmendem Maße möchten EDV-Anwender heute elektronische Dokumente über unsichere Netze (Telefonnetz, Internet) versenden. Es stellt aus technischer Sicht kein Problem dar, ein im Klartext vorliegendes (d. h. insbesondere unverschlüsseltes) elektronisches Dokument auf seinem Weg vom Absender zum Empfänger zu verfälschen oder gar den Absender zu fälschen. Dennoch soll der Empfänger absolut verläßlich prüfen können, ob ein erhaltenes elektronisches Dokument tatsächlich vom angegebenen Absender stammt und auf dem Weg zum Empfänger nicht verändert wurde. Darüber hinaus möchte der Empfänger im Streitfalle Dritten gegenüber beweisen können, daß er ein bestimmtes Dokument von einer bestimmten Person/Institution erhalten hat. Dies erfordert sozusagen ein elektronisches Analogon zu der konventionellen handschriftlichen Unterschrift. Die Kryptographie bietet hier eine Lösung: sogenannte digitale Signaturverfahren. Mittels digitaler Signatur soll dem Empfänger eines Dokuments ein rechtsverbindlicher Beweis dafür geliefert werden, daß das Dokument auch tatsächlich vom ausgewiesenen Sender stammt und auf dem Übertragungswege nicht verfälscht wurde. Umgekehrt hat der Sender ein Interesse an einem solchen Beweis dahingehend, daß der richtige Empfänger das Dokument auch unverfälscht erhalten hat. Zur Gewährleistung der Sicherheit, d. h. der Unverfälschbarkeit einer digitalen Signatur müssen insbesondere folgende Bedingungen erfüllt sein:

1. Der Secret Key des Benutzers, der die mathematische Funktion zum Signieren eines elektronischen Dokumentes parametrisiert, muß absolut geheim bleiben.
2. Der Algorithmus zum Signieren eines Dokumentes darf nicht manipulierbar sein. Er wird in einer sicheren physikalischen Umgebung (z. B. durch eine Chipkarte) ausgeführt.
3. Der Benutzer muß sich sicher sein, daß er genau das von ihm gewünschte Dokument signiert und nichts anderes.

Wegen der Bedingungen 1 und 2 stimmen Experten darin überein, daß der Secret Key des Benutzers im von außen nicht zugänglichen Bereich einer Chipkarte gespeichert werden sollte, welche über die Fähigkeit verfügt, mit Hilfe dieses Keys die digitale Signatur zu einem vorgegebenen Dokument zu berechnen. Ein Lösungsvorschlag, der zudem noch Bedingung 3 erfüllt, ist derzeit noch nicht bekanntgeworden.

Das typische derzeit für die Praxis favorisierte System zum Signieren elektronischer Dokumente zeigt ein Dokument auf einem Monitor oder Display an, worauf der Benutzer (menügesteuert) den Befehl gibt, dieses Dokument durch seine Chipkarte signieren zu lassen. Ob dann tatsächlich das zuvor angezeigte Dokument signiert wird, ist allerdings nicht gewährleistet, denn der benutzte Computer könnte so manipuliert sein, daß der an den Computer angeschlossene Chipkartenleser zum Signieren ein Dokument erhält, welches sich von dem zuvor am Monitor oder Display angezeigten – vielleicht nur geringfügig – unterscheidet.

Hiervon ausgehend liegt der Erfindung die Aufgabe zugrunde, die Vorrichtung der genannten Art dahingehend weiterzubilden, daß der Benutzer sicher sein kann, daß er genau das von ihm gewünschte Dokument signiert und nichts anderes. Die Vorrichtung soll mit geringem Aufwand das bislang ungelöste Teilproblem, welches auch als Darstellungsproblem bezeichnet wird, beim fälschungssicheren Signieren elektronischer Dokumente mit einem geringen Aufwand lösen. Ferner soll die Vorrichtung für den Anwender in einfacher Weise durchschaubar sein und eine einfache Anordnung der zum Einsatz gelangenden peripheren Hardwarekomponenten ermöglichen.

Die Lösung dieser Aufgabe erfolgt gemäß den im Patentanspruch 1 angegebenen Merkmalen.

Die vorgeschlagene Vorrichtung zeichnet sich durch einen einfachen und funktionsgerechten Aufbau aus und löst in zweckmäßiger Weise das Darstellungsproblem bei der Erzeugung digitaler Signaturen. Durch die Durchschaubarkeit der einfachen Steueranordnung und der verwendeten peripheren Hardwarekomponenten ist es für den Computeranwender ohne weiteres ersichtlich, daß das sichere signierende Modul, wie insbesondere die Chipkarte und das Chipkartenterminal, genau die gleichen Daten oder Signale als Eingabe erhält wie das genannte externe Ausgabegerät. Das sichere Modul, welches den zum Signieren notwendigen Secret Key dauerhaft speichert und welches mit Hilfe dieses Secret Keys die digitale Signatur eines vorgegebenen elektronischen Dokuments oder einer vorgegebenen Datei berechnet und diesem definiert zuordnet, wird in zweckmäßiger Weise zwischen den Computer, und zwar insbesondere dessen Zentraleinheit, und das externe Ausgabegerät geschaltet. Darüber hinaus ist das zwischengeschaltete sichere Modul derart ausgebildet, daß erfindungsgemäß die Korrektheit einer vorgegebenen digitalen Signatur für ein vorgegebenes elektronisches Dokument überprüfbar ist. Das Ausgabegerät kann als Monitor bzw. Display oder als Drucker bzw. Plotter ausgebildet sein. Das sichere Modul und das Ausgabegerät sind über bevorzugt frei verlegte sichtbare Datenkabel und eine Kopplungskomponente derart miteinander verbunden, daß das sichere Modul und das externe Ausgabegerät stets die gleichen Daten empfangen. Die Kopplungskomponente, welche in zweckmäßiger Weise als ein T-Stück zur Verbindung der Datenkabel ausgebildet sein kann, besitzt keine weiteren Fähigkeiten, als das Weiterleiten der vom Computer erhaltenen Daten an die beiden Ausgänge, die auf das sichere Modul und ferner auf das externe Ausgabegerät geführt sind.

In einer besonderen Weiterbildung der Erfindung ist ein Druckertreiber für Postscriptdrucker derart vorgesehen, daß mit der Ausgabe eines Druckbefehls, insbesondere einer Postscriptdatei, in dem sicheren Modul die Durchführung der Signatur der zugeordneten Datei erfolgt, welche vom Drucker ausgegeben wird.

Besondere Ausgestaltungen und Weiterbildungen der Erfindung sind in den Unteransprüchen sowie der weiteren Beschreibung eines besonderen Ausführungsbeispiels angegeben.

Fig. 1 zeigt schematisch ein Blockschaltbild der Vorrichtung mit einem sicheren Modul **2**, welches den zum Signieren eines Dokuments notwendigen Secret Key dauerhaft speichert. Das sichere Modul ermöglicht ferner mittels des genannten Secret Keys die digitale Signatur für ein elektronisches Dokument oder eine vorgegebene Datei. Das genannte Dokument bzw. die Datei wird mittels eines Computers **4**, insbesondere dessen Zentraleinheit, bereitgestellt und zu einem externen Ausgabegerät über eine bevorzugt frei verlegte und/oder sichtbare Datenleitung **8** geleitet. Das Ausgabegerät **6** dient zur Ausgabe der Daten in sichtbarer Form und ist als Monitor bzw. Display oder Drucker bzw. Plotter ausgebildet. Das sichere Modul **2** ist zwischen dem Computer **4** und dem Ausgabegerät **6** installiert und enthält parallel zu diesem exakt die gleichen Daten oder Dateien wie das externe Ausgabegerät **6**. In zweckmäßiger Weise ist die Datenleitung **8** für einen Benutzer sichtbar als Kabel ver-

legt, und zwar vorzugsweise als konventionelles Druckerkabel oder Monitorkabel. Für den Anwender ist somit unmittelbar aufgrund der einfachen Verbindung der externen Komponenten erkennbar, daß in das externe Ausgabegerät die gleichen Daten gelangen wie in das sichere Modul, welches zwischen der Zentraleinheit des Computers und dem externen Ausgabegerät **6** installiert ist. Das zwischengeschaltete sichere Modul **2** ist in besonders zweckmäßiger Weise zur Überprüfung einer vorgegebenen digitalen Signatur für ein vorgegebenes elektronisches Dokument ausgebildet.

In bevorzugter Weise enthält das sichere signierende Modul **2** einerseits eine Prozessorchipkarte, in welcher insbesondere der Secret Key gespeichert ist, und andererseits ein Chipkartenterminal **12** zum Ansteuern der Chipkarte **10**. Das Modul **2** ermöglicht erfindungsgemäß ferner, in der beschriebenen Anordnung die Korrektheit einer vorgegebenen digitalen Signatur für ein vorgegebenes elektronisches Dokument zu überprüfen.

In besonders zweckmäßiger Weise erfolgt die Verbindung des Computers **4** bzw. dessen zentralen Einheit mit dem sicheren Modul **2** sowie dem externen Ausgabegerät **6** über eine Kopplungskomponente **14**. Es handelt sich hierbei um eine passive Kopplungskomponente, vorzugsweise in Form eines T-Stücks, welches einerseits an die mit dem Computer **2** verbundenen Datenleitung **8** angeschlossen ist und dessen Ausgänge **16, 18** andererseits über Datenleitungen **20, 22** mit dem externen Ausgabegerät **6** bzw. dem Modul **2** verbunden sind. Die Kopplungskomponente **14** besitzt keine weiteren Fähigkeiten als das Weiterleiten der vom Computer **4** eingehenden Daten an die beiden Ausgänge **16, 18** und über die Kabel **20, 22** zum externen Ausgabegerät **6** sowie zum Modul **2** bzw. Chipkartenterminal **12**. Für einen Anwender ist somit aufgrund der Einfachheit der Kopplungskomponente, welche keine weitere oder andere Funktionalität als das Weiterleiten der vom Computer **4** erhaltenen Daten an das Ausgabegerät **6** sowie an das das sichere Modul **2** aufweist, unmittelbar erkennbar, daß die gleichen Daten des Computers **4** sowohl an das Modul **2** als auch an das Ausgabegerät **6** gelangen.

In einer besonderen Weiterbildung ist dem Computer **4** ein Druckertreiber **24** zugeordnet, welcher einen üblichen Druckertreiber ersetzt. Der erfindungsgemäße Druckertreiber **24** ist derart ausgebildet, daß mit Ausgabe eines Druckbefehls, insbesondere für eine Postscript-Datei, in dem sicheren Modul **2** die Durchführung der Signatur der nachfolgenden Datei initiiert wird, welche auf dem externen Ausgabegerät bzw. Drucker **6** über den Ausgang **16** und die Datenleitung **20** ausgegeben wird.

Bezugszeichenliste

2 sicheres Modul
4 Computer
6 Ausgabegerät
8 Datenleitung
10 Prozessorchipkarte
12 Chipkartenterminal
14 Kopplungskomponente
16, 18 Ausgang
20, 22 Datenleitung/Kabel
24 Druckertreiber

Patentansprüche

1. Vorrichtung zum Erstellen einer digitalen Signatur, enthaltend einen Computer (4) und ein externes Ausgabegerät (6), **dadurch gekennzeichnet**, daß zwischen dem Computer (4), insbesondere dessen Zentraleinheit, und dem externen Ausgabegerät (6) ein sicheres Modul (2) angeordnet ist, zur Berechnung der digitalen Signatur mit Hilfe eines Secret Key.

2. Vorrichtung nach Anspruch 1, dadurch gekennzeichnet, daß das sichere Modul (2) ein Chipkartenterminal (12) sowie eine Prozessorchipkarte (10) zum dauerhaften Speichern des Secret Key enthält.

3. Vorrichtung nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß mit dem Computer (4) eine Kopplungskomponente (14) verbunden ist, deren Ausgänge (16, 18) zum einen auf das externe Ausgabegerät (6) und zum anderen auf das sichere Modul (2), insbesondere über Datenleitungen oder Kabel (20, 22) geführt sind.

4. Vorrichtung nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, daß bevorzugt über die Kopplungskomponente (14) das Ausgabegerät (6) und das sichere Modul (2) derart miteinander verbunden sind, daß das Ausgabegerät (6) und das sichere Modul (2) immer die gleichen Daten vom Computer (4) empfangen.

5. Vorrichtung nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, daß der Computer (4) einen derart ausgebildeten Druckertreiber enthält, daß mit der Ausgabe eines Druckbefehls im sicheren Modul (2) insbesondere im Chipkartenterminal (12) die Durchführung der Signatur der vom Computer (4) mit dem Druckbefehl ausgegebenen Datei initiiert wird.

Hierzu 1 Seite(n) Zeichnungen

Nummer:
Int. Cl.[6]:
Offenlegungstag:

DE 198 11 720 A1
H 04 L 9/32
30. September 1999